

**Übersetzungsbüro - Translation Office – Bureau de Traduction**

Detlef W. Petzold

Postfach 13 02 – 88153 Lindenberg/Allgäu, Germany/Allemagne

Tel. & Fax: 0 83 81 – 94 14 99

E-Mail: dwp-uebersetzungsbuero@web.de

---

**C E R T I F I C A T E**

This is to certify that the enclosed documents are, to the best of my knowledge and understanding, a true and correct translation of the German copies into English.


Detlef Petzold

Übersetzungsbüro

Am Wunderbrunnen 9

88161 Lindenberg / Allg.

Tel.+Fax: 08381 / 94-14-99



Öffentlich bestellter und  
beidogter Übersetzer für  
die englische Sprache

Public certified and sworn  
English Language Translator

Lindenberg/Allgäu (Germany)

May 16, 2008

**T-Mobil**

**Telefax**

**Recipient** T214

**Please pass  
on to** Dr. Sinning

**Tel. No.** -2225

**No. of pages  
(including  
cover page)** 6

**Person to  
contact** Dr. Thomas Breitbach, System Security

**Tel. No.** 0228/936-3315, Telefax: 0228/936-3398

**Date** January 14, 1999

**Subject** Report of Invention

Dear Mr. Sinning:

Enclosed to the present letter you will find a Report of Invention relating to Mobile Radio Banking.

This subject matter has already been briefly discussed between Mr. Maringer and you. The Report of Invention of those other participants will be submitted later.

Should you have any questions I would be pleased to be at your disposal.

Very truly yours,

(signature)  
Thomas Breitbach

If an invention becomes known externally this will result in a loss of protectability.

Receipt of the report/communication of invention at the patents/trademarks/licenses division will be regarded as receipt of said report/communication of invention only.

DeTeMobil Deutsche Telekom Mobil Net GmbH, Landgrabenweg 151, 53227 Bonn

Personal statements:

Name: Breitbach	Personal No.: 323179
First name: Thomas	Position: T211
Academic title: Dr.	Internal company position: SB
Tel.: 0228/936-3315	Telefax: 0228/936-3398
Sphere of responsibility: System Security	Nationality: German
Participation in the invention (in %): 33.33	
Private address: Kolpingstr. 23a, 56645 Nickenich	

I report the following invention:

1. Title of the invention:  
Standardized Mobile Radio Banking Services
2. The following members of the T-Mobil staff participate in the invention

2<sup>nd</sup> inventor:

Name: Maringer	Personal No.: 31125
First name: Günter	Position: T243
Academic title: Dr.	Internal company position: FL
Tel.: 0228/936-1249	Telefax: 0228/936-3309
Sphere of responsibility: Chip Card Systems	Nationality: German
Participation in the invention (in %): 33.33	
Private address: Troschelstr. 8, 53115 Bonn	

3<sup>rd</sup> inventor:

Name: Conrad	Personal No.: 30122
First name: Alan	Position: M221
Academic title:	Internal company position: SB
Tel.: 0228/936-2712	Telefax: 0228/935-882712
Sphere of responsibility: Product Managem.	Nationality: British

Participation in the invention (in %): 33.33

Private address: Freie Bitze 24, 53639 Königswinter

Name: Thomas Breitbach

---

3. The following external persons participate in the invention:

---

Name, company /

---

4. The problem of the invention is as follows:

---

For the time being the HBCI standard of the German economy based on credit offers the possibility to offer home banking by means of a bank-overlapping standard. A concept to offer these services also by means of a mobile telephone is suggested by this invention.

---

5. The invention is regarded as being service-bound (Para 54 ArbEG), i.e.: (x)  
that the invention was made during the duration of employment relationship;  
that the invention originates from the sphere of responsibility of the employee;  
that the invention is substantially based on experience or work of the company.  
The invention is regarded as being non service-bound (Paras 18, 19 ArbEG) ( )
- 

6. It is intended to publish the invention
- a) provisionally not (x)
- b) as a printed publication ( )  
name of the publication organization  
date of publication
- c) publication by lecture ( )  
place of event  
date of event
- 

7. The following documents are included for the preparation of a right of use application (if possible, one copy in the name of all inventors only):

- a) description of prior art with bibliography data statement (x)
- b) description of advantages compared with the prior art (x)

- c) exact and detailed description of the action of the invention (x)  
d) manual sketches, circuit diagrams, drawings ( )  
e) if necessary, measuring records, technical reports ( )
- 

8. Development of the invention:

I have been induced to make the invention

- a) because the employer has set a task and advised the way to find a solution; ( )  
b) because the employer has set a task and did not advise the way to find a solution; ( )  
c) however, the employer did not set a task but the way was found because, based on the fact that I am a member of the company, I knew defects and requirements not determined on my own; ( )  
d) however, the employer did not set a task but the way was found because, based on the fact that I am a member of the company, I knew defects and requirements determined on my own;  
e) because I/we have set a task within the scope of my/our field of duties; (x)  
f) because I/we have set a task outside the scope of my/our duties. ( )
- 

9. Solution of the problem (it is possible to give more than one answer):

- a) The solution was found on the basis of well-known professional considerations. (x)  
b) The solution was found on the basis of work or experiences of the employee. ( )  
c) Technical auxiliary means of the employee were used. ( )
- 

10. The invention has been submitted as a proposal for improvement.

(x) no ( ) yes; if known, state WgNr.

---

I affirm that no other persons than those mentioned in this document have participated in the development of the invention and that I have no knowledge of any prior use or publication of the invention.

---

Place, Date

01-14-99 Bonn

Signature of the inventor Thomas Breitbach

---

**T-Mobil**

**Telefax**

**Recipient** Office of Riebling

**Please pass  
on to** Mr. Stoinsky

**Tel. No.** 08382/78027

**No. of pages  
(including  
cover page)** 10

**Person to  
contact** Dr. Günter Maringer, T2

**Tel. No.** (0228) 936-1249, Telefax: (0228) 936-881249

**Date** February 12, 1999

**Subject** „Standardized Mobile Radio Banking Services“

Dear Mr. Stoinsky:

As regards the above matter you requested us to provide additional information. The document enclosed to the present letter explains the concept in detail.

Should you have any questions I would be pleased to be at your disposal.

Very truly yours,

DeTeMobil  
Deutsche Telekom MobilNet GmbH

(signature)  
G. Maringer

**T-MOBIL**

**DRAFT**

**Technical Draft**

**Standardized Mobile Radio Banking Services**

**Version 0.0.3  
February 9, 1999**

**CONFIDENTIAL**

**T Mobil**

**Deutsche Telekom MobilNet GmbH  
Landgrabenweg 151  
D-53227 Bonn**

**© DeTeMobil Deutsche Telekom MobilNet GmbH 1999**

Passing on or copying of this document, use or communication of its contents or its storage on data carriers of any kind whatsoever is allowed neither completely nor in extracts to the extent that this has not been allowed in writing explicitly. Contraventions enjoin payment of damages. All rights reserved. (Protection note DeTeMobil GmbH)



**Revision History**

Version	Date	Reason for Revision
0.0.1	02-29-1999	Headword collection, Thomas Breitbach
0.0.2	02-05-1999	Revision, document combination Thomas Breitbach, Günther Maringer
0.0.3	02-09-1999	First review Thomas Breitbach, Günther Maringer, Alan Conrad

<b>1 INTRODUCTION</b>	<b>4</b>
<b>2 PRODUCT IDEA</b>	<b>4</b>
<b>3 INFRASTRUCTURE</b>	<b>6</b>
<b>4 SECURITY</b>	<b>7</b>

## 1 INTRODUCTION

In the form of a general view this document describes the concept of safe GSM mobile radio banking services by use of the open HBCI standard. In the scope of a cooperation between cooperative bank associations and T-Mobil the technical drafts shall be put into action.

First of all the product idea as well as the customer process are roughly described in this document. The safety draft included in Chapter 4 of this document and the distribution of the cryptographical keys required form a focal point of the document.

## 2 PRODUCT IDEA

For banking services demands paperless, comfortable ways of submission are inquired increasingly. Because of the effect of rationalization to be achieved by this this development is supported by the banks. However, the very small penetration of PC online accesses of less than ten percent (10%) presents an obstacle in Germany first of all.

The mobile radio with approximately 15,000,000 customers and high growth rates is much more common. This is a possible key for a mass market-capable electronical access to banking transactions. In addition, the customer is offered the possibility to obtain a mobile access to banking transactions as well. Instead of the PC the chip card accepts the role of the customer either as far as the user dialogue or the safety functions are concerned. This will be allowed by a new standardized technology named SAT (SIM Application Toolkit) which allows the mobile chip card to assume the role of control of services.

Within the German banking world the HBCI standard will be the platform for home banking purposes. Therefore, it is obvious to apply this standard also in the context of mobile radio-supported banking activities. Unfortunately the HBCI protocol developed for the internet is too extensive for direct copying on today's GSM mobile radio world. This concerns either the bandwidth necessary for data transmission or memory capacity and computing capacity required on the side of the customer (SIM card).

Therefore, there is a trace existing to carry out a transformation between the HBCI used by banks and a compressed HBCI to be defined on the side of the mobile radio. It is the problem of such transforming component - hereafter called HBCI gateway - to reduce data to be transmitted to a GSM-compatible extent. Therefore, the basic idea is that both the SIM card and the computer of the bank communicate explicitly with the HBCI gateway directly, which HBCI gateway accepts a proxy function.

This transformation of the protocol is regarded as being an evolutionary step on the way to an end-to-end HBCI. It is to be expected that the bandwidth of mobile radio networks will increase as such that, on a medium-term, this appears to be a realistic target to be achieved.

The transformation mentioned results also in a transformation of safety mechanisms used: While the HBCI protocol is used between the gateway and the banking world an own safety protocol will be used from the side of GSM. The suggestion submitted as follows is based on the RDH variant for HBCI and on a symmetrical triple DES solution on the side of GSM.

The following figure illustrates the facts in a simple way:

(Figures)

The GSM standard encoding will be used at the GSM air interface. Above it there is a triple DES encoding on the application level, which triple DES encoding ensures the distance between SIM card and HBCI gateway. The distance between HBCI gateway and bank is subject to the standard HBCI protocol and the RDH variant.

Since the HBCI gateway assumes safety-relevant functions it is expected that it is operated in bank computing centres.

To secure the distance between HBCI gateway and SIM card it is necessary to define a secret key between gateway and SIM card. To ensure that the key will absolutely be kept secret it is suggested to use a method, where the bank sends an initialing PIN to the customer by a PIN letter which is to be entered into the mobile telephone by the customer once. With the help of a suitable algorithm the key will be derived from the SIM as well as from the HBCI gateway. Based on this method it is ensured that third parties do not have any knowledge to this key. This safety philosophy is described in Chapter 4 in detail.

## **2.1 Business Transactions**

In a first step it is suggested to offer the following business transactions: *account inquiry, latest transactions, and remittance orders.*

## **2.2 Operating Interface**

All actions will be initiated by the user by means of the operating control of the mobile telephone. For this purpose an own menu point, i.e. „mobile banking“, is set by the SIM card. After having clicked here submenus are offered, i.e. „account“, „transactions“, and „configuration“.

The limited possibilities of a mobile telephone keyboard require an own optimized user guidance. In particular, for this reason the own bank connection is stored in the card so that it is necessary to input this bank connection only once.

On this occasion it should be considered that, in numerous cases, there are customers who keep several accounts in a bank. Therefore, a suitable selection possibility should be offered.

To ensure that unauthorized persons are unable to arrange for banking transactions a PIN should be enquired on the occasion of each transaction demand. This PIN will be managed by the card locally.

### *Account inquiry*

after having clicked this menu point:

- inquiry of account (selection from list)
- inquiry of PIN
- customer is informed of account balance

### *Transactions*

after having clicked this menu point:

- inquiry of account (selection from list)
- inquiry of PIN
- customer is informed of latest transactions

### *Remittance*

after having clicked this menu point:

- inquiry of account (selection from list)
- inquiry of remittance account
- inquiry of bank code for remittance purposes
- inquiry of amount
- inquiry of intended purpose
- inquiry of PIN
- customer receives confirmation by SMS

### *Configuration*

after having clicked this menu point:

- SMS recipient address of HBCI gateway
- inquiry of bank code and own account numbers (maximum of „n“ accounts)
- inquiry or initialization PIN (see above, 20 decimal digits + check number for input mistake findings)
- inquiry of PIN

Data input are stored in the card then. In addition, menu points „show“ and „delete“ are offered.

## **3 PROTOCOLS**

### **3.1.1 Subscription**

Banking services activation is effected after having clicked menu point „configuration“ (see above); bank code and account numbers of own accounts as well as initialization PIN and local PIN for use of banking services are inquired then. Own

banking connection data are stored on the card. Based on the initialization PIN the card calculates a Ksms key to ensure the communication between HBCI GSM gateway and SIM card (see Chapter 4). The inquiry of the local (card) PIN serves for protection against unauthorized subscription attempts.

Following the calculation of Ksms the SIM card reports the subscription wish to the HBCI gateway. Then the local key generation follows at the HBCI gateway and the first dialogue with the HBCI banking system is carried out then. Furthermore, the HBCI gateway sends a message to the card which causes adjustment of the banking menu title and complete activation of the application.

### 3.2 Business Transactions

Suitable message forms are to be defined for individual business transactions. In any case the messages are encoded with the help of Ksms.

## 4 Security

Security is a very important requirement for the product described here. Above all it is the aim of the security concept to avoid misuse (*authentication of the customer*). Furthermore, it is important to guarantee the confidentiality of data transmitted (*encoding of transmission*). Both requirements are realized by means of cryptographical methods.

### 4.1 Role Model

Basically the following roles may be identified with this concept:

- (1) customer
- (2) network provider
- (3) HBCI gateway provider
- (4) HBCI credit bank system provider (computing centre of the bank)

For security reasons roles (3) and (4) should dispose of a distinct confidential relationship. In principle the provider of the HBCI gateway is able to monitor or draw up messages falsely. Therefore, it would be meaningful if the provider of the HBCI gateway originates from the ambient banking field.

### 4.2 Security Areas

The entire distance from the mobile telephone of the customer to the HBCI server of the bank is divided into two security areas. The first area extends from the SAT SIM card to the HBCI gateway, and the distance from the HBCI gateway to the bank server is the second security area.

#### 4.3 Security Area 1: From SAT SIM to HBCI gateway

Basically the security functions of this area are determined by assignment and use of a special Ksms key. With the help of this 128 bit triple DES key all messages exchanged between the SAT SIM and the HBCI gateway are encoded.

Ksms ensures the connection from the SIM to the HBCI gateway. The Ksms authenticates either customer or HBCI gateway and is also used to encode this distance. The Ksms is a special key of the banking application and remains hidden to the network provider. To guarantee this the following method is used for generation purposes:

*Upon card personalization and together with the banking application the network provider applies a KIV, a master key, on all cards to generate the customer-specific Ksms. Prior to subscription of the service the customer receives the data of his/her bank inclusive of a 20 digit PIN. Upon initialization of the SAT application (online subscription) the proper customer key Ksms is generated from the PIN with the help of KIV (encoding of the PIN, bank code, and account number per triple DES with the help of KIV serving as a key).*

*For the generation of Ksms in the HBCI gateway the PIN must also be passed on to the gateway provider. An option is to generate the PIN at the HBCI gateway and pass it on to the bank.*

The authentication of both roles, i.e. customer and HBCI gateway, is carried out through knowledge of the PIN exchanged in writing. In addition, the master key KIV must be exchanged between the network provider and the HBCI gateway provider. Therefore, this master key authenticates the HBCI gateway in addition.

As an option the following additional authentication of the customer may be made on the basis of the identification signal of his/her mobile connection:

*GSM connections are secured (GSM 02.09) with the help of a special key (Ki). The evaluation of calling line identification (CLI) of the SAT SIM sent may be made at the HBCI gateway. For this purpose the D1 telephone number must be managed in the HBCI gateway.*

#### 4.4 Security Area 2: From the HBCI Gateway to the Credit Institution System

An unmodified HBCI protocol will be used on the interface between HBCI gateway and bank. For the development of this interface, see (HBCI2). In the development illustrated in this document the RDH variant is used.

In the HBCI specification model the HBCI gateway represents the customer system. Public and private signature keys and codes are stored on the HBCI gateway for each customer.

The mechanism of the authentication of public customer and banking keys must be included in a contractual agreement between the provider of the HBCI gateway and the provider of the bank server. Should there be no implicated confidential relationship existing between these parties Ini letters or even certificates may be used.

#### 4.5 Overall View of Keys used

key	use	Generation	depository	crypto method key length	knowledge by	remark
Ki	GSM authentication of air interface	Network provider on card personalization	SIM authentication centre of network provider	proprietary symmetric 128 bit	network provider	
Kc	GSM encoding of air interface	network + SIM on call set-up	mobile telephone + GSM network	A5 54 bits	network provider	
CKpub	HBCI public key (encoding) of customer	HBCI gateway on subscription	HBCI gateway bank	RSA 768 bits	gateway provider, bank	
CKpriv	HBCI private key (encoding) of customer	HBCI gateway on subscription	HBCI gateway	RSA 768 bits	gateway provider	
AKpub	HBCI public key (authentication) of customer	HBCI gateway on subscription	HBCI gateway, bank	RSA 768 bits	gateway provider	
AKpriv	HBCI private key (authentication) of customer	HBCI gateway on subscription	HBCI gateway	RSA 768 bits	gateway provider	
CBpub	HBCI public key (encoding) of bank		Bank, HBCI gateway	RSA 768 bits	gateway provider, bank	
CBpriv	HBCI private key (encoding) of bank		Bank	RSA 768 bits	bank	
ABpub	HBCI public key (authentication) of bank		Bank, HBCI gateway	RSA 768 bits	gateway provider, bank	



ABpriv	HBCI private key (authentication) of bank		Bank	RSA 768 bits	bank	
KIV	master key for generation of Ksms	network provider	SIM card	triple DES (2-key) 128 bits	SIM card, HBCI gateway	auxiliary key of Ksms by means of PIN; master key identical for all customers
Ksms	encoding and SAT SIM authentication to gateway	HBCI gateway prior to subscription and SAT SIM on subscription	HBCI gateway SAT SIM	triple DES (2-key) 128 bits	gateway provider, customer also indirectly	Ksms is generated in card following PIN input

#### 4.6 Overall View

The present technical draft offers a high security level. The participating technical components (SIM, mobile telephone, HBCI gateway) are by far less susceptible against misuse compared with a PC of a customer. Based on the view of the customer a new service is offered with the present technical draft which offers a high safety standard at the same time.

### 5 Prospect

The concept described in this document represents a possible starting point for services in the entire „Mobile Electronic Commerce" field. In the medium and long run it will be possible to extend the concept as follows:

- extension by push services, i.e. communications or transactions initiated by credit institutions;
- support of a second card slots (Dual Slot Mobiles) and, as a basis, involvement of the money card (transactions and loading activities)

### 6 References

(HBCI2) Homebanking Computer Interface, Interface Specification, Version 2.0.1 of February 2, 1998

Bundesverband deutscher Banken e.V., Deutscher Sparkassen- und Giroverband e.V., Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Verband öffentlicher Banken e.V. (Hrsg.)

(GSM 02.09) European Digital Cellular Telecommunication systems (Phase 2);  
Security Aspects (GSM 02.09)  
European Telecommunications Standards Institute 1994

**T-Mobil**

**Telefax**

**Recipient** Patent Attorney Dr.-Ing. Peter Riebling

**Tel. No.** 08382-78027

**No. of pages**  
**(including**  
**cover pages)** 2

**Person to**  
**contact** Cécile Leloup (comm. Patent Division), T214

**Tel. No.** 0228/936-1229, Telefax 0228/936-2225

**Date** February 1, 1999

**Subject** Order

Our Ref. T99002 DE

Dear Dr. Riebling:

For the preparation of patent application documents, please find enclosed another invention made in our company.

Working title:  
„Standardized Mobile Radio Banking Services“

The inventors can be reached as follows:

- 1.) Dr. Breitbach, Tel. 0228/936-3315 (Telefax: -3398)
- 2.) Mr. Conrad, Tel. 0228/936-2712 (Telefax: -882712)
- 3.) Dr. Maringer, Tel. 0228/936-1249 (Telefax: - 3309)

Very truly yours,

DeTeMobil  
Deutsche Telekom MobilNet GmbH  
- Patents/Trademarks/Licenses Division -

i.A.  
(signature)  
Dr. Richard Sinning

i.A.  
(signature)  
Cécile Leloup

Enclosures  
Invention Documents

### **Prior Art**

HBCI (Home Banking Computer Interface) is a method developed by the German economy based on credit for bank-overlapping home banking by using, for example, a personal computer (PC) and a fixed network modem.

### **Advantages of the Invention compared with the Prior Art**

Apart from home computers the invention allows to use mobile telephones as a customer-related HBCI platform without using any accessory devices.

### **Exact and detailed Description of the operating Method of the Invention**

HBCI is based on a cryptographical end-to-end security between a chip card or floppy disk on the side of the customer and the banking server. The distribution of the customer HBCI system on two components, i.e. the GSM SIM card and a HBCI gateway, is the basis of this invention. A direct use of the HBCI protocol up to the GSM SIM card is out of question both because of reasons of capacity and due to the session-orientated alignment of the HBCI protocol. Two transmitting ranges are formed between the SIM card and the HBCI gateway, and a cryptographical security is realized on both ranges.

The HBCI gateway is added to the transmitting path which depacks the HBCI protocol, converts the protocol flow as such that a compatibility with the GSM SIM card (with, for example, the short message service or GPRS as a carrier service) is obtained. Finally the HBCI gateway exchanges the converted protocol with customer-used SIM card. From the bank server's point of view a standard-conforming HBCI protocol is used completely: The security defined through HBCI is used between the banking server and the HBCI gateway. A new safety protocol is used between HBCI gateway and SIM card. This corresponds to a data amount-reduced but HBCI-equivalent protocol from the security point of view.

In addition, the invention is characterized by the fact that a method will be used which allows to safely generate and store cryptographical keys in the SIM card following SIM card personalization. For this purpose the HBCI gateway generates a special PIN letter. Input of the PIN in the mobile telephone generates the customer-specific key in the SIM card. In this manner a safe, encoded communication path is set up between HBCI gateway and SIM card without hazard through „man in the middle“ attacks (e.g. the network provider).